PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-112851
(43)Date of publication of application : 28.04.1998

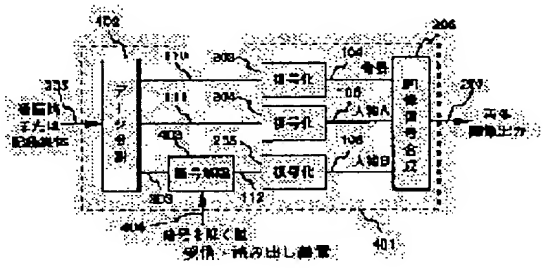
(51)Int.Cl. H04N 7/167
H04L 9/36
H04N 7/24

(21)Application number : 08-265740
(22)Date of filing : 07.10.1996

(71)Applicant : HITACHI LTD
(72)Inventor : NAKAYA YUICHIRO
MITSUSAKA SATOSHI

(54) METHOD AND DEVICE FOR TRANSMITTING OR RECORDING IMAGE INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a fixed information without a decryption key by applying encryption processing to truly important parts in an image and making the other parts visible.
SOLUTION: A multiplex bit stream 305 is given to a data division section 402, in which the stream is divided into bit streams 110, 111, 303. Each bit stream is incorporated with identification information denoting whether or not encryption is required. The coded streams 110, 111 are given to decoding sections 203, 204 and the stream 303 is given to a decryption section 403, where cryptographic is decrypted by using a key 404 and the resulting bit stream 112 is fed to a decoding section 205. When a reproduction is not available of the key 404, the stream 303 cannot be decrypted but the streams 110, 111 are correctly reproduced. Since other information than a person B denoted by the stream 303 is correctly reproduced, the user can obtain limited information from an incompletely reproduced image regardless of possession of no key.



LEGAL STATUS
[Date of request for examination] 01.10.2001
[Date of sending the examiner's decision of rejection] 29.06.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3834364
[Date of registration] 28.07.2006
[Number of appeal against examiner's decision of rejection] 2004-015462
[Date of requesting appeal against examiner's decision of rejection] 26.07.2004
[Date of extinction of right]

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1] Transmission or the record approach of image information characterized by multiplexing and outputting the coding bit stream about all bodies after performing coding processing independently for every body in an image to subject-copy image information and adding processing of encryption only to the coding bit stream about one specific piece or two or more specific bodies.
[Claim 2] The coding bit stream enciphered although the coding bit stream which is not enciphered was correctly reproduced when beginning to receive or read the image information outputted according to the approach of claim 1 and reproducing is the image reconstruction approach characterized by being correctly unreproducible if there is no key which solves a code.
[Claim 3] Transmission or the recording device of image information characterized by to multiplex and output the coding bit stream about all bodies after adding processing of encryption only to the coding bit stream about one specific piece or two or more specific bodies in the information which had a means perform coding processing independently for every body in an image to subject-copy image information, and a means perform encryption processing to information, and was encoded by the above-mentioned coding means.
[Claim 4] the picture reproducer characterized by the body corresponding to the enciphered coding bit stream being correctly unreproducible if there is no key although it has a means carries out reception or reading appearance of the image information outputted according to the approach of claim 1, and reproduce, and a means reproduce the enciphered information using the key which solves a code and the body corresponding to the coding bit stream which is not enciphered reproduces correctly.
[Claim 5] It is transmission or the record approach of written ********** to claim 1 characterized by adding processing of encryption to coincidence to the coding bit stream about one or less body.
[Claim 6] Transmission or the record approach of image information according to claim 1 characterized by adding processing of encryption to coincidence to the coding bit stream about two or less bodies.
[Claim 7] It is transmission or the record approach of claim 1 to which the minimum is also characterized by surely enciphering the coding bit stream about one body while outputting the coding bit stream, or image information given in 5 or 6.
[Claim 8] Transmission or the record approach of image information according to claim 1, 5, 6, or 7 characterized by not fixing the body with which the coding bit stream is enciphered, but being switched according to time amount.
[Claim 9] Transmission or the recording device of image information according to claim 3 characterized by adding processing of encryption at the coding bit stream about one or less body at coincidence.
[Claim 10] Transmission or the recording device of image information according to claim 3 characterized by adding processing of encryption at the coding bit stream about two or less bodies at coincidence.
[Claim 11] Transmission or the recording device of claim 3 characterized by the minimum surely adding processing of encryption to the coding bit stream about one body, or image information given in 9 or 10.
[Claim 12] Transmission or the recording device of image information according to claim 3, 9, 10, or 11 characterized by switching the target body in case processing of encryption is added to an objective coding bit stream.
[Claim 13] Picture reproducer according to claim 4 characterized by the body corresponding to one or less enciphered coding bit stream being correctly reproducible to coincidence.
[Claim 14] Picture reproducer according to claim 4 characterized by the body corresponding to two or less enciphered coding bit streams being correctly reproducible to coincidence.
[Claim 15] Claim 4 characterized by the body corresponding to the coding bit stream enciphered by switching the coding bit stream which adds processing of code discharge to the information outputted according to transmission or the record approach of image information according to claim 8 being correctly reproducible, or picture reproducer given in 13 or 14.

[Claim 16] The record medium which recorded the image information recorded according to claims 1 or 5 or the approach of 6 or 7.
[Claim 17] The communication link, the broadcast, database, or video-on-demand system of an image constituted by claim 3, 9 or 10, or 11 or 12 with transmission or the recording device of the image information of a publication, and picture reproducer according to claim 4, 13, 14, or 15.
[Claim 18] The communication link, the broadcast, database, or video-on-demand system of an image according to claim 17 characterized by specifying the upper limit of a number although enciphered in the coding bit stream about a body.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to transmission, the record, and the playback approach of image information in pictorial communication, broadcast, and database system.
[0002]
[Description of the Prior Art] By advance of an electron device technique etc., an image and voice are digitized and, generally transmission and accumulating are coming to carry out. With original information, since there is very much amount of information, information, such as an image and voice, is transmitted or accumulated as a coding bit stream in many cases, after compressing using an information-compression technique (coding). At this time, in order to perform image reconstruction correctly, a coding and playback side needs to adopt a common image coding method. For this reason, methods, such as H.261, MPEG1, and MPEG 2, are already defined as international standards of an image coding method.
[0003] MPEG4 is in one of the image coding methods with which the current standardization activity is done. Incorporating the new function which was not in an old standard coding method is considered by this method. Content-based coding is in one of them. This is a technique aiming at making edit, composition, etc. of an image easy to process by encoding the body in an image independently. The example of drawing 1 and the terminal which processes Content-based coding to 2 is shown. The part shown by the common number points out the same thing. First, at the terminal 101 for transmission / record of drawing 1 , field division is processed by the field division section 103 to the subject-copy picture signal 102 of an input. For example, in the field division section, an image is divided into three signals of the signals 105 and 106 of a part with which the signal 104 of a part with which the background was reflected, and each two persons were reflected noting that the image with which the person binary name and the background were reflected as an input was given. In addition, field division is not performed to the input image of one sheet, but there is also a method of incorporating a required part separately from two or more images. To this signal by which field division was carried out, processing of coding is performed in the coding sections 107, 108, and 109, respectively, and the coding bit streams 110, 111, and 112 are outputted. Of course about this processing, the one coding processing section may encode three parts separately instead of having two or more coding processing sections (the coding processing section will perform coding processing 3 times in this case). The encoded bit stream is multiplexed in the multiplexing section 113, and is outputted to a channel or are recording equipment as one coding bit stream 114.
[0004] In reception and the read-out terminal 201 of drawing 2 , data division of the coding bit stream 114 read from reception or are recording equipment is carried out in the data division section 202 from a channel at the coding bit streams 110, 111, and 112 of each part. These bit streams are decrypted in the decryption sections

203, 204, and 205, respectively, and acquire the picture signals 104, 105, and 106 showing each part. These picture signals are again compounded as an image of one sheet in the picture signal composition section 206, and the playback picture signal 207 is outputted.
[0005] Although the example which is a reception and read-out side as it is, and reproduces the picture signal which is transmission / record side and was inputted was taken up in drawing 1 and 2, Content-based coding was not devised for the purpose of carrying out such [originally] usage. In Content-based coding, since the body in an image is encoded separately, a specific body can be deleted and added or zooming and deforming edit processing can be performed for a coding bit stream. On the other hand, in H.261, MPEG1, and MPEG 2 which are the conventional coding method, coding is performed by making the small block in an image into a unit, and, generally the boundary line of this small block is not in agreement with the profile of the body in an image. For this reason, in order to perform the above-mentioned edit processing, the encoded image information must once be decrypted to an analog signal.
[0006]
[Problem(s) to be Solved by the Invention] As long as there is no key of a solving-code sake, it becomes impossible to see all the range of an image, if the encoded image information is enciphered.
[0007]
[Means for Solving the Problem] By Content-based coding, an image is encoded and encryption is processed only to the information about a specific body. In case the information encoded by this approach is reproduced, some images become possible [seeing] even when there is no key for decryption. Moreover, encryption can be effectively processed by switching the body which adds processing of encryption, without increasing throughput (= complexity of a terminal).
[0008]
[Embodiment of the Invention] In charged broadcast of analog television broadcasting, CATV, etc., in case a TV signal is enciphered, the method called the Rhine rotation is used well. This is the technique (the sequence of a signal is replaced, and the contents are not understood and are carried out) of scrambling a picture signal in the same Rhine (scanning line). Since the user (subscriber) who has paid the tariff has a key for solving this scramble, he can reproduce a right image. On the other hand, since the addressee (non-subscriber) who has not paid the tariff cannot solve a scramble, he cannot see a right image. However, if constraint is prepared in the violence of a scramble (for example, constraint is prepared in a gap of the location of the signal scramble before and after a scramble), even if the scramble has started, slight information can be acquired from the reproduced image. It is said that this "slight information" has the effectiveness of producing the volition which joins a non-subscriber.
[0009] On the other hand, when enciphering and transmitting the digitized image information, how to encipher and transmit the encoded bit stream can be considered. However, the addressee without the key for usually solving a code in this case cannot see image information included in the coding bit stream which received at all. The bit stream by which, as for this, the code is not solved is because it becomes the information which is completely meaningless for the decryption machine of an accepting station. Since this is prevented, how to encode and transmit the picture signal to which the scramble was once applied can be considered. However, by this approach, since the statistical property of the picture signal after applying a scramble changes from the usual picture signal a lot, the problem to which the rate of an information compression in coding falls occurs.
[0010] The example of the transmission and the recording device 301 which performs coding and encryption processing to drawing 3 by the approach of this invention is shown. The part shown by drawing 1 and the common number has pointed out the same thing. Processing of field division is performed in the field division section 103 to the subject-copy picture signal 102 of an input. Suppose that an image is divided into three parts of the parts 104 and 105 to which a background 106 and each two persons were reflected noting that the image with which the person binary name and the background were reflected as an input was given like the case of drawing 1 . To each of this signal by which field division was carried out, processing of coding is performed in the coding sections 107, 108, and 109, and the coding bit streams 110, 111, and 112 are outputted. Although the coding bit streams 110 and 111 are supplied to the multiplexing section 304 as they are like the case of drawing 1 , the coding bit stream 112 containing the information about Person B is supplied to the multiplexing section as an encryption bit stream 303, after being enciphered using the encryption key 306 in the encryption section 302. The information for identifying whether the coding bit streams 110, 111, and 112 are bit streams as which he is enciphered, respectively at this time is incorporated, and this information is utilized in case it is playback. In this way, the multiplexed bit stream 305 is outputted to a channel or are recording equipment.
[0011] Drawing 4 shows the example of a configuration of the reception and the read-out equipment 401 to the

bit stream transmitted or recorded with the equipment of drawing 3 . The part shown by drawing 1 , and 2, 3 and a common number has pointed out the same thing. After the multiplexing bit stream 305 is received or read, in the data division section 402, data division of it is carried out at three bit streams 110, 111, and 303. The identification information which shows whether the bit stream is enciphered is included in each coding bit stream. Then, while this equipment supplies the coding bit streams 110 and 111 to the decryption sections 203 and 204 as they are, the enciphered coding bit stream 303 is supplied to the code discharge section 403, and cancels a code using the key 404 for solving a code here. The key 404 and encryption key (306 of drawing 3) for solving a code may differ from the case of being the same, with the cipher system adopted. The coding bit stream 112 which is the output of the code discharge section is supplied to the decryption machine 205. The picture signals 104, 105, and 106 which are the outputs of three decryption machines are compounded in the picture signal composition section 206, and acquire the playback picture signal 207.

[0012] The above is processing in the case of having key information for a playback side solving a code. On the other hand, when a playback side does not have this key, a code cannot be solved correctly. It becomes impossible therefore, to reproduce correctly the picture signal 106 about the person B of drawing 4 . However, since it is correctly reproducible, the signal 104 about a background and the signal 105 about Person A are correctly reproduced by the output image finally obtained except Person B. For this reason, although a user does not have a key, he becomes possible [acquiring the information limited from the image reproduced imperfectly].

[0013] The transmission and the recording apparatus, and the reception and read-out equipment which were explained to be drawing 3 by 4 can be used as communication link / broadcast system and a database (video on demand) structure-of-a-system element. In this case, the key for solving a code is distributed only to a subscriber. On the other hand, since a non-subscriber can acquire the limited information about broadcast and the image information currently transmitted or recorded, it becomes easy to make a judgment whether it joins or not. In the pay-per-view system which pays a tariff for especially every program, a judgment whether a tariff is paid or not is made frequently. Therefore, the function which reproduces an image imperfectly is effective also in the semantics which mitigates the burden by the side of the user who judges.

[0014] In a video-on-demand system, when reading the information recorded, for example on the server of a remote place through a charged public network, a user has to pay traffic. For this reason, in spite of being unable to see an image at all, it is hard to think that a user without a key accesses this information specially. However, if the approach shown by this invention is used, since [as which a user without a key also regards some images at least] things can be carried out, possibility of accessing the information enciphered even if it paid communication link costs will become high. This is effective, also when leading also to performing advertisement to a non-subscriber effectively and increasing a subscriber.

[0015] The body which generally appears in an image changes with time amount, and the importance for every body changes with situations on that occasion. Therefore, when the body (for example, specific characters) enciphered is fixed, possibility of becoming inadequate [the semantics of the effectiveness of encryption] is high. This problem can cope with it by switching the body enciphered. However, if it is going to encipher many bodies to coincidence, the throughput of encryption or code discharge will increase, and the problem to which a terminal becomes intricately and expensive occurs. How to restrict the number of the bodies enciphered by coincidence as realistic countermeasures over this problem can be considered. In performing processing of encryption or code discharge in hardware, it stops the number of an encryption machine and code discharge machines, or it becomes possible to realize processing also with comparatively low speed equipment. Moreover, since processing speed demanded also when performing this processing by software can be made low, low speed CPU realizes processing or it becomes possible to turn the part by which a leeway was given in processing speed to other processings.

[0016] Transmission of the image whose number of the bodies enciphered by drawing 5 is always one or less, or the example of a configuration of a recording device 501 is shown. The part shown by drawing 1 -4 and the common number has pointed out the same thing. Processing of field division is performed in the field division section 103 to the subject-copy picture signal 102 of an input. The outputs 104, 105, and 106 of the field division section are the picture signals about the body by which field division was carried out, respectively like the case of drawing 1 . To each of this signal by which field division was carried out, processing of coding is performed in the coding sections 107, 108, and 109, and the coding bit streams 110, 111, and 112 are outputted. These coding bit streams are inputted into a transfer switch 502. This transfer switch is controlled so that the coding bit stream about the body below a piece always passes the encryption section 303. Processing of encryption is performed by the encryption key information 306 in the encryption section. Therefore, below the

piece will always be enciphered in the output bit streams 503, 504, and 505 of a transfer switch. This information is supplied to the data multiplexing section 506, and the multiplexing bit stream 507 is outputted to a channel or a recording device. In addition, the identification information of whether the code of the bit stream is carried out is included in the coding bit stream for every body like before. Moreover, it is thought that the approach of performing manually is the most effective, considering the effectiveness of the encryption to a viewer, when real time nature is not required especially concerning the processing which chooses the body to encipher. When this real time nature is not required, in an image database or a video-on-demand system, the case where the coded-image information for recording on a recording device is created etc. corresponds.

[0017] Drawing 6 shows the example of a configuration of the reception and the read-out equipment 601 to the bit stream transmitted or recorded with the equipment of drawing 5 . The part shown by drawing 1 -5 and the common number has pointed out the same thing. After the multiplexing bit stream 507 is received or read, in the data division section 602, data division of it is carried out at three bit streams 503, 504, and 505. The identification information which shows whether the bit stream is enciphered is included in each coding bit stream. A transfer switch 603 supplies below the piece in three bit streams to the code discharge section 403 based on this recognition signal. In the code discharge section, a code is canceled using the information 404 about the key which solves a code. In this way, the obtained coding bit streams 110, 111, and 112 are decrypted with the decryption vessels 204, 205, and 206. The picture signals 104, 105, and 106 which are the outputs of each decryption machine are compounded in the picture signal composition section 206, and acquire the playback picture signal 207.

[0018] At this time, although this equipment is enciphered in the coding bit stream about the body inputted, it knows in advance that a number is always one or less piece. Unless such an agreement exists in beforehand between a coding side and a playback side, since it corresponds when the worst (when many bit streams are enciphered), a playback side must have the capacity to cancel the code of many coding bit streams to coincidence. Therefore, the constraint about the number of bit streams with which the above is enciphered is effective when reducing the throughput of simplification of the hardware of a terminal, or the software of a terminal.

[0019]

[Effect of the Invention] By this invention, when the enciphered digital image information is received, it becomes possible truly within an image to see except an important part to be processed [of encryption], and the transmitting person of image information can offer fixed information also to an addressee without the key which solves a code.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing having shown the example of a configuration of the image transmission and the recording device which performs Content-based coding.

[Drawing 2] It is drawing having shown the example of a configuration of the picture reproducer which performs reception and read-out of the image information encoded by Content-based coding.

[Drawing 3] It is drawing having shown the example of a configuration of the image transmission and the recording device which performs encryption processing to the specific body in an image.

[Drawing 4] It is drawing having shown the example of a configuration of the picture reproducer which performs reception and read-out of the image information to which encryption processing was performed to the specific

body in an image.
[Drawing 5] It is drawing having shown the example of a configuration of the image transmission and the recording device which performs encryption processing, switching the target body to the body below the piece in an image.
[Drawing 6] It is drawing having shown the example of a configuration of the picture reproducer which performs reception and read-out of the image information to which encryption processing was performed, switching the target body to the body below the piece in an image.
[Description of Notations]
101 -- Transmission and the recording device of the image information based on Content-based coding, 102 -- Subject-copy image information, 103 -- The field division section, 104 -- The picture signal about a background, 105 -- The picture signal about Person A, 106 -- The picture signal about Person B, 107, 108, 109 -- The image coding section, 110 -- The coding bit stream about a background, 111 -- The coding bit stream about Person A, 112 -- The coding bit stream about Person B, 113, 304, 506 -- The data multiplexing section, 114 -- Multiplexing bit stream, 201 -- Reception and read-out equipment of the image information based on Content-based coding, 202, 402, 602 -- The data division section, 203, 204, 205 -- Image decryption section, 206 -- The picture signal composition section, 207 -- A playback image output, 301 -- Transmission and the recording device of the image information based on Content-based coding with an encryption function, 302 -- The encryption section, 303 -- The enciphered coding bit stream about Person B, 305 507 -- The multiplexing bit stream, 306 which were enciphered -- Key information for encryption, 401 -- Reception and read-out equipment of the image information based on Content-based coding with a code discharge function, 403 [Transmission and the recording device of the image information based on coding,] -- The code discharge section, 404 -- The key information for solving a code, 501 -- Content-based with the function to perform **** encryption which switches an object object 502 603 -- A bit stream transfer switch, 503, 504, 505 -- The coding bit stream which switched application/object for unsuitable [of encryption], 601 -- Content-based with the function to perform **** code discharge which switches an object object Reception and read-out equipment of the image information based on coding.

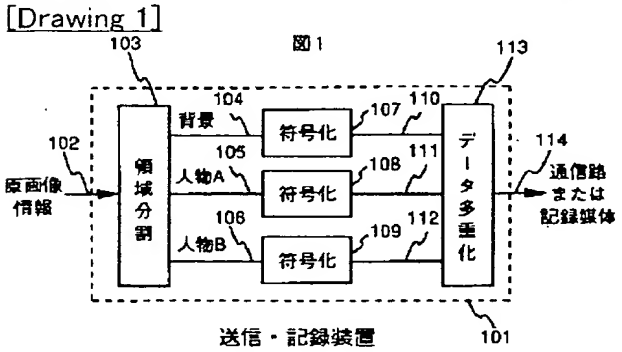
[Translation done.]

* NOTICES *

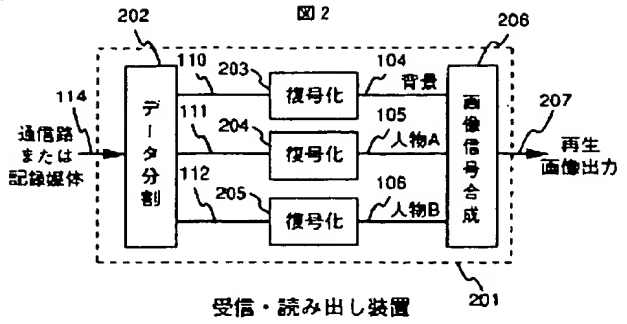
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

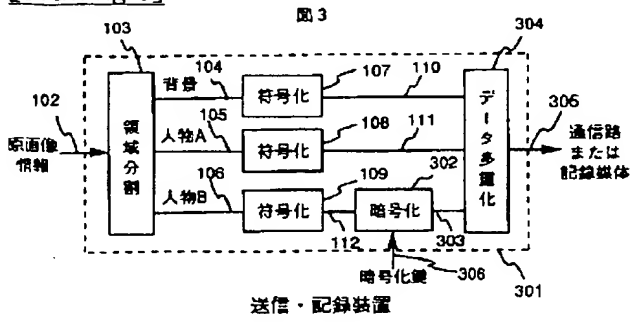
[Drawing 1]



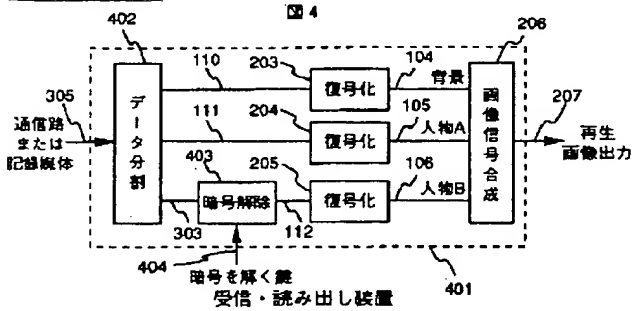
[Drawing 2]



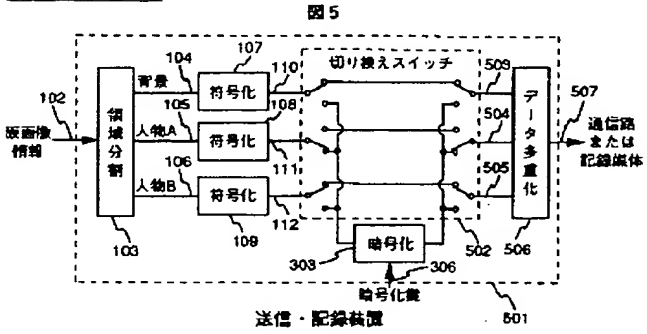
[Drawing 3]



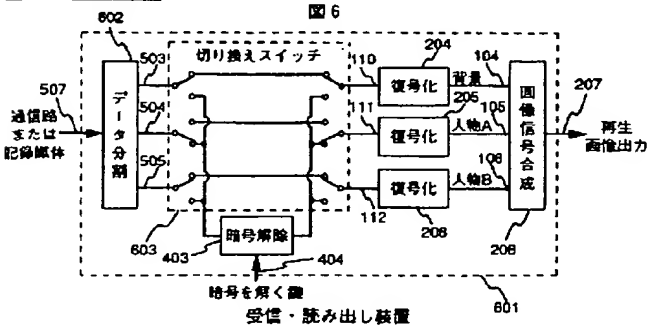
[Drawing 4]



[Drawing 5]



[Drawing 6]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－112851

(43)公開日　平成10年(1998)４月28日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｎ	7/167	Ｈ０４Ｎ	7/167	Ｚ
Ｈ０４Ｌ	9/36	Ｈ０４Ｌ	9/00	６８５
Ｈ０４Ｎ	7/24	Ｈ０４Ｎ	7/13	Ｚ

審査請求　未請求　請求項の数18　ＯＬ　（全６頁）

(21)出願番号　特願平8－265740

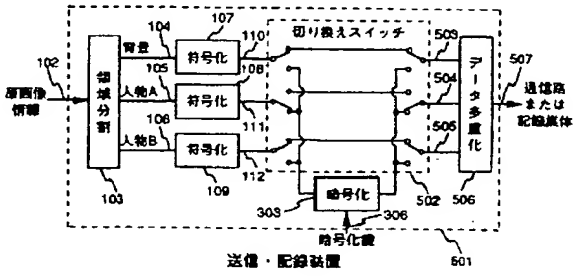
(22)出願日　平成８年(1996)10月７日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　中屋　雄一郎
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　三坂　智
東京都国分寺市東恋ケ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　画像情報の伝送または記録方法および装置

(57)【要約】
【課題】　符号化されたディジタル画像を暗号化して伝送した場合、受信側が暗号を解くための鍵をもっていないと再生画像をまったく見ることができなくなる問題を解決する。
【解決手段】　対象画像をContent-based codingによって物体ごとに独立に符号化し、画像内の特定の物体に関する符号化ビットストリームに対してのみ暗号化の処理を加え、暗号化されたビットストリームに変換した後に多重化して伝送または記録する。
【効果】　暗号を解くための鍵を持たない受信者も伝送された画像の一部を再生することが可能となり、限定された情報を得ることができる。

図5



1

【特許請求の範囲】

【請求項１】原画像情報に対して画像内の物体ごとに独立に符号化処理を行い、特定の１個または複数の物体に関する符号化ビットストリームのみに暗号化の処理を加えた後に全物体に関する符号化ビットストリームを多重化して出力することを特徴とする画像情報の伝送または記録方法。

【請求項２】請求項１の方法に従って出力された画像情報を受信または読み出して再生する際に、暗号化されていない符号化ビットストリームは正しく再生するが、暗号化された符号化ビットストリームは暗号を解く鍵がないと正しく再生することができないことを特徴とする画像再生方法。

【請求項３】原画像情報に対して画像内の物体ごとに独立に符号化処理を行う手段と、情報に対して暗号化処理を行う手段を持ち、上記符号化手段によって符号化された情報の中で特定の１個または複数の物体に関する符号化ビットストリームのみに暗号化の処理を加えた後に全物体に関する符号化ビットストリームを多重化して出力することを特徴とする画像情報の伝送または記録装置。

【請求項４】請求項１の方法に従って出力された画像情報を受信または読み出して再生する手段と、暗号化された情報を暗号を解く鍵を用いて再生する手段を持ち、暗号化されていない符号化ビットストリームに対応する物体は正しく再生するが、暗号化された符号化ビットストリームに対応する物体は鍵がないと正しく再生することができないことを特徴とする画像再生装置。

【請求項５】同時に１個以下の物体に関する符号化ビットストリームに対して暗号化の処理を加えることを特徴とする請求項１に記載び画像情報の伝送または記録方法。

【請求項６】同時に２個以下の物体に関する符号化ビットストリームに対して暗号化の処理を加えることを特徴とする請求項１に記載の画像情報の伝送または記録方法。

【請求項７】符号化ビットストリームを出力している間は最低でも１個の物体に関する符号化ビットストリームが必ず暗号化されていることを特徴とする請求項１または５または６に記載の画像情報の伝送または記録方法。

【請求項８】符号化ビットストリームが暗号化されている物体が固定されておらず、時間に応じて切り換えられることを特徴とする請求項１または５または６または７に記載の画像情報の伝送または記録方法。

【請求項９】同時に１個以下の物体に関する符号化ビットストリームに暗号化の処理を加えることを特徴とする請求項３に記載の画像情報の伝送または記録装置。

【請求項１０】同時に２個以下の物体に関する符号化ビットストリームに暗号化の処理を加えることを特徴とする請求項３に記載の画像情報の伝送または記録装置。

【請求項１１】最低でも１個の物体に関する符号化ビットストリームに必ず暗号化の処理を加えることを特徴とする請求項３または９または１０に記載の画像情報の伝送または記録装置。

2

【請求項１２】物体の符号化ビットストリームに暗号化の処理を加える際に、対象となる物体を切り換えられることを特徴とする請求項３または９または１０または１１に記載の画像情報の伝送または記録装置。

【請求項１３】同時に１個以下の暗号化された符号化ビットストリームに対応する物体を正しく再生できることを特徴とする請求項４に記載の画像再生装置。

【請求項１４】同時に２個以下の暗号化された符号化ビットストリームに対応する物体を正しく再生できることを特徴とする請求項４に記載の画像再生装置。

【請求項１５】請求項８に記載の画像情報の伝送または記録方法にしたがって出力された情報に対し、暗号解除の処理を加える符号化ビットストリームを切り換えることによって暗号化された符号化ビットストリームに対応する物体を正しく再生することができることを特徴とする請求項４または１３または１４に記載の画像再生装置。

【請求項１６】請求項１または５または６または７の方法に従って記録された画像情報を記録した記録媒体。

【請求項１７】請求項３または９または１０または１１または１２に記載の画像情報の伝送または記録装置と、請求項４または１３または１４または１５に記載の画像再生装置によって構成される画像の通信または放送またはデータベースまたはビデオオンデマンドシステム。

【請求項１８】物体に関する符号化ビットストリームの中で暗号化されているものの数の上限が規定されていることを特徴とする請求項１７に記載の画像の通信または放送またはデータベースまたはビデオオンデマンドシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、画像通信・放送・データベースシステムにおける画像情報の伝送・記録および再生方法に関するものである。

【０００２】

【従来の技術】電子デバイス技術の進歩などにより、映像や音声をディジタル化して伝送・蓄積することが一般的に行われるようになりつつある。映像や音声などの情報は原情報のままでは情報量がきわめて多いため、情報圧縮技術を用いて圧縮（符号化）した後に符号化ビットストリームとして伝送あるいは蓄積される場合が多い。このとき、画像再生を正しく行うためには符号化側と再生側が共通の画像符号化方式を採用する必要がある。このため、画像符号化方式の国際標準としてＨ．２６１、ＭＰＥＧ１、ＭＰＥＧ２などの方式が既に定められている。

【０００３】現在標準化作業が進められている画像符号

化方式の一つにＭＰＥＧ４がある。この方式では、これまでの標準符号化方式にはなかった新しい機能を盛り込むことが検討されている。その一つにContent-based codingがある。これは、画像内の物体を独立に符号化することによって、画像の編集・合成などの処理を行いやすくすることを目的とした技術である。図１と２にContent-based codingの処理を行う端末の例を示す。共通の番号で示される部分は同じものを指す。まず、図１の送信・記録用端末１０１では、入力の原画像信号１０２に対して領域分割部１０３で領域分割の処理を行う。例えば入力として人物２名と背景が写った画像が与えられたとして、領域分割部では背景が写った部分の信号１０４および２人の人物それぞれが写った部分の信号１０５、１０６の３個の信号に画像が分けられる。なお、１枚の入力画像に対して領域分割を行うのではなく、複数の画像から必要な部分を別々に取り込む方法もある。この領域分割された信号に対して、符号化部１０７、１０８、１０９でそれぞれ符号化の処理が行われ、符号化ビットストリーム１１０、１１１、１１２が出力される。もちろんこの処理に関しては、複数の符号化処理部を持つ代わりに１個の符号化処理部が別々に３個の部分を符号化しても良い（この場合、符号化処理部は３回符号化処理を行うことになる）。符号化されたビットストリームは多重化部１１３で多重化され、一つの符号化ビットストリーム１１４として通信路または蓄積装置へと出力される。

【０００４】図２の受信・読み出し端末２０１では、通信路から受信または蓄積装置から読み出された符号化ビットストリーム１１４を、データ分割部２０２で各部分の符号化ビットストリーム１１０、１１１、１１２にデータ分割する。これらのビットストリームは復号化部２０３、２０４、２０５でそれぞれ復号化され、各部分を表す画像信号１０４、１０５、１０６を得る。これらの画像信号は画像信号合成部２０６で再び１枚の画像として合成され、再生画像信号２０７が出力される。

【０００５】図１と２では、送信・記録側で入力された画像信号をそのまま受信・読み出し側で再生する例を取り上げたが、Content-based codingは本来このような使い方をすることを目的として考案されたものではない。Content-based codingでは画像内の物体が別々に符号化されているため、特定の物体を削除・追加したり拡大・縮小・変形したりする編集処理を符号化ビットストリームを対象に行うことができる。これに対して従来の符号化方式であるＨ．２６１、ＭＰＥＧ１、ＭＰＥＧ２では、画像内の小ブロックを単位として符号化が行われており、一般的にこの小ブロックの境界線は画像内の物体の輪郭とは一致していない。このため、上記の編集処理を行うためには符号化された画像情報を一旦アナログ信号に復号化しなければならない。

【０００６】

【発明が解決しようとする課題】符号化された画像情報を暗号化してしまうと、暗号を解くのための鍵がない限り画像の全範囲を見ることができなくなる。

【０００７】

【課題を解決するための手段】Content-based codingによって画像を符号化し、特定の物体に関する情報のみに対して暗号化の処理を行う。この方法によって符号化された情報を再生する際には、暗号解読のための鍵がない場合でも画像の一部は見ることが可能となる。また、暗号化の処理を加える物体を切り換えることにより、処理量（＝端末の複雑さ）を増やすことなく効果的に暗号化の処理を行うことができる。

【０００８】

【発明の実施の形態】アナログテレビ放送やCATVなどの有料放送では、テレビ信号を暗号化する際にラインローテーションと呼ばれる方式が良く利用されている。これは、画像信号を同一ライン（走査線）内でスクランブルする（信号の順番を入れ替えて内容をわからなくする）手法である。料金を支払っている利用者（加入者）は、このスクランブルを解くための鍵を持っているため、正しい画像を再生することが可能である。一方、料金を払っていない受信者（非加入者）は、スクランブルを解くことができないために正しい画像を見ることができない。しかし、スクランブルの激しさに制約を設ければ（例えばスクランブル前とスクランブル後の信号の位置のずれに制約を設ける）、たとえスクランブルがかかっていても、再生された画像からわずかの情報を得ることができる。この「わずかの情報」が、非加入者に加入する意欲を生じさせる効果を持っていると言われている。

【０００９】一方、ディジタル化した画像情報を暗号化して伝送する場合、符号化されたビットストリームを暗号化して伝送する方法が考えられる。しかしこの場合、通常は暗号を解くための鍵を持たない受信者は受信した符号化ビットストリームに入っている画像情報を全く見ることができない。これは、暗号が解かれていないビットストリームは受信端末の復号化器にとっては全く意味の無い情報となってしまうためである。これを防ぐため、一旦スクランブルをかけた画像信号を符号化して伝送する方法が考えられる。しかし、この方法ではスクランブルをかけた後の画像信号の統計的性質が通常の画像信号から大きく変化してしまうため、符号化における情報圧縮率が低下する問題が発生する。

【００１０】図３に本発明の方法により符号化および暗号化処理を行う送信・記録装置３０１の例を示す。図１と共通の番号により示される部分は同じものを指している。入力の原画像信号１０２に対して領域分割部１０３で領域分割の処理が行われる。図１の場合と同様に、入力として人物２名と背景が写った画像が与えられたとして、背景１０６および２人の人物それぞれが写った部分１０４、１０５の３個の部分に画像が分割されるとす

る。この領域分割された信号それぞれに対して、符号化部１０７、１０８、１０９で符号化の処理が行われ、符号化ビットストリーム１１０、１１１、１１２が出力される。符号化ビットストリーム１１０と１１１は図１の場合と同様にそのまま多重化部３０４に供給されるが、人物Ｂに関する情報が入っている符号化ビットストリーム１１２は暗号化部３０２で暗号化鍵３０６を用いて暗号化された後に暗号化ビットストリーム３０３として多重化部に供給される。このとき符号化ビットストリーム１１０、１１１、１１２はそれぞれ自分自身が暗号化されているビットストリームであるかを識別するための情報が組み込まれており、再生の際にはこの情報が活用される。こうして多重化されたビットストリーム３０５は通信路または蓄積装置へと出力される。

【００１１】図４は図３の装置で送信または記録されたビットストリームに対する受信・読み出し装置４０１の構成例を示している。図１、２、３と共通の番号により示される部分は同じものを指している。多重化ビットストリーム３０５は受信または読み出された後、データ分割部４０２において３個のビットストリーム１１０、１１１、３０３にデータ分割される。それぞれの符号化ビットストリームにはそのビットストリームが暗号化されているか否かを示す識別情報が組み込まれている。そこでこの装置は符号化ビットストリーム１１０と１１１はそのまま復号化部２０３と２０４に供給する一方で、暗号化された符号化ビットストリーム３０３は暗号解除部４０３に供給し、ここで暗号を解くための鍵４０４を利用して暗号を解除する。暗号を解くための鍵４０４と暗号化鍵（図３の３０６）は、採用されている暗号化方式によって同一である場合と異なる場合がある。暗号解除部の出力である符号化ビットストリーム１１２は復号化器２０５に供給される。３個の復号化器の出力である画像信号１０４、１０５、１０６は画像信号合成部２０６において合成され、再生画像信号２０７を得る。

【００１２】以上は再生側が暗号を解くための鍵情報を持っている場合の処理である。これに対し、再生側がこの鍵を持たない場合には暗号を正しく解くことができない。したがって、図４の人物Ｂに関する画像信号１０６を正しく再生することができなくなる。しかし、背景に関する信号１０４と人物Ａに関する信号１０５は正しく再生することができるため、最終的に得られる出力画像では人物Ｂ以外は正しく再生される。このため、利用者は鍵を持たないにもかかわらず、不完全に再生された画像から限定された情報を得ることが可能となる。

【００１３】図３と４で説明した送信・記録装置と受信・読み出し装置は、通信・放送システムおよびデータベース（ビデオオンデマンド）システムの構成要素として使用することができる。この場合、暗号を解くための鍵は加入者にのみ配布される。一方、非加入者は放送・伝送または記録されている画像情報に関する限定された情報を得ることができるため、加入するか否かの判断が行いやすくなる。特に番組ごとに料金を支払うペイパービューシステムでは、料金を支払うか否かの判断は頻繁に行われる。したがって、不完全に画像を再生する機能は判断を行う利用者側の負担を軽減する意味でも有効である。

【００１４】ビデオオンデマンドシステムでは、例えば遠隔地のサーバに記録された情報を有料の公衆網を通じて読み出す場合に利用者は通信費を負担しなければならない。このため、画像をまったく見ることができないにもかかわらず、鍵を持たない利用者がこの情報にわざわざアクセスするとは考えにくい。しかし、本発明で示した方法を利用すれば、鍵を持たない利用者も少なくとも画像の一部を見ることできるため、通信費用を負担してでも暗号化された情報にアクセスする可能性が高くなる。このことは、非加入者に対する宣伝を効果的に行うことにもつながり、加入者を増やす上でも効果的である。

【００１５】一般に画像に登場する物体は時間と共に変化し、かつその場の状況によって物体ごとの重要性は変化する。したがって、暗号化される物体（例えば特定の登場人物）を固定しておくと暗号化の効果という意味で不十分となる可能性が高い。この問題は暗号化される物体を切り換えることによって対処することができる。しかし、同時に多数の物体を暗号化しようとすると暗号化や暗号解除の処理量が増加し、端末が複雑、高価になってしまう問題が発生する。この問題に対する現実的な対応策として、同時に暗号化される物体の数を制限する方法が考えられる。暗号化や暗号解除の処理をハードウェア的に行う場合には暗号化器、暗号解除器の数を抑えたり、比較的低速な装置でも処理を実現することが可能になる。また、ソフトウェア的にこの処理を行う場合も要求される処理速度を低くすることができるため、より低速なＣＰＵによって処理を実現したり、処理速度に余裕ができた分を他の処理に廻すことが可能となる。

【００１６】図５に暗号化される物体の数が常に１個以下である画像の伝送または記録装置５０１の構成例を示す。図１～４と共通の番号により示される部分は同じものを指している。入力の原画像信号１０２に対して領域分割部１０３で領域分割の処理が行われる。図１の場合と同様に、領域分割部の出力１０４、１０５、１０６はそれぞれ領域分割された物体に関する画像信号である。この領域分割された信号それぞれに対して、符号化部１０７、１０８、１０９で符号化の処理が行われ、符号化ビットストリーム１１０、１１１、１１２が出力される。これらの符号化ビットストリームは切り換えスイッチ５０２に入力される。この切り換えスイッチは常に一個以下の物体に関する符号化ビットストリームが暗号化部３０３を通過するように制御される。暗号化部では、暗号化鍵情報３０６により暗号化の処理が行われる。し

たがって、切り換えスイッチの出力ビットストリーム５０３、５０４、５０５の中で常に一個以下が暗号化されていることになる。この情報はデータ多重化部５０６に供給され、多重化ビットストリーム５０７が通信路または記録装置に出力される。なお、これまでと同様に物体ごとの符号化ビットストリームにはそのビットストリームが暗号されているか否かの識別情報が組み込まれる。また、暗号化する物体の選択を行う処理に関しては、特にリアルタイム性が要求されない場合には視聴者への暗号化の効果を考えながら手動で行う方法が最も効果的であると考えられる。このリアルタイム性が要求されない場合には、画像データベースやビデオオンデマンドシステムにおいて、記録装置に記録するための符号化画像情報を作成する場合などが相当する。

【００１７】図６は図５の装置で送信または記録されたビットストリームに対する受信・読み出し装置６０１の構成例を示している。図１～５と共通の番号により示される部分は同じものを指している。多重化ビットストリーム５０７は受信または読み出された後、データ分割部６０２において３個のビットストリーム５０３、５０４、５０５にデータ分割される。それぞれの符号化ビットストリームにはそのビットストリームが暗号化されているか否かを示す識別情報が組み込まれている。この識別信号を元に切り換えスイッチ６０３は３個のビットストリームの中の一個以下を暗号解除部４０３に供給する。暗号解除部では、暗号を解く鍵に関する情報４０４を用いて暗号が解除される。こうして得られた符号化ビットストリーム１１０、１１１、１１２は復号化器２０４、２０５、２０６で復号化される。各復号化器の出力である画像信号１０４、１０５、１０６は画像信号合成部２０６において合成され、再生画像信号２０７を得る。

【００１８】このとき、この装置は入力される物体に関する符号化ビットストリームの中で暗号化されているものの数が常に１個以下であることを事前に知っている。このような取り決めが事前に符号化側と再生側の間に存在しない限り、再生側は最悪の場合（多数のビットストリームが暗号化されている場合）に対応するために多数の符号化ビットストリームの暗号を同時に解除する能力を持たなければならない。したがって上記の暗号化されているビットストリームの数に関する制約は、端末のハードウェアの簡略化、あるいは端末のソフトウェアの処理量を減らす上で有効である。

【００１９】

【発明の効果】本発明により、暗号化されたディジタル画像情報を受信した場合、画像内で本当に暗号化の処理が必要である重要な部分以外は見ることが可能となり、画像情報の送信者は暗号を解く鍵を持たない受信者に対しても一定の情報を提供することができる。

【図面の簡単な説明】

【図１】Content-based codingを行う画像送信・記録装置の構成例を示した図である。

【図２】Content-based codingによって符号化された画像情報の受信・読み出しを行う画像再生装置の構成例を示した図である。

【図３】画像内の特定の物体に対して暗号化処理を行う画像送信・記録装置の構成例を示した図である。

【図４】画像内の特定の物体に対して暗号化処理が行われた画像情報の受信・読み出しを行う画像再生装置の構成例を示した図である。

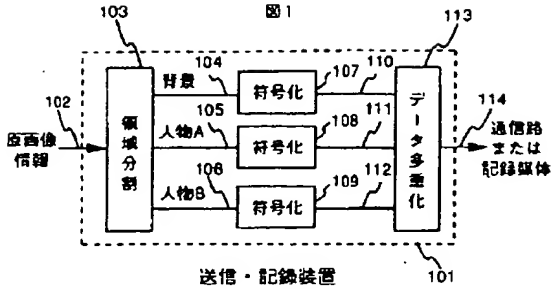
【図５】画像内の一個以下の物体に対し、対象となる物体を切り換えながら暗号化処理を行う画像送信・記録装置の構成例を示した図である。

【図６】画像内の一個以下の物体に対し、対象となる物体を切り換えながら暗号化処理が行われた画像情報の受信・読み出しを行う画像再生装置の構成例を示した図である。

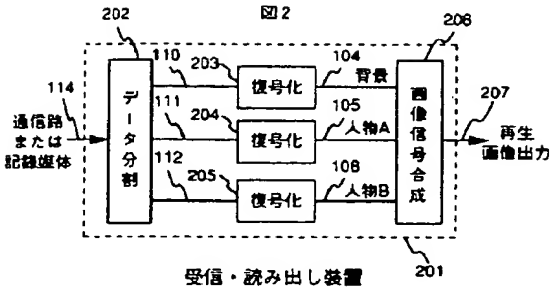
【符号の説明】

１０１…Content-based codingに基づく画像情報の送信・記録装置、１０２…原画像情報、１０３…領域分割部、１０４…背景に関する画像信号、１０５…人物Ａに関する画像信号、１０６…人物Ｂに関する画像信号、１０７、１０８、１０９…画像符号化部、１１０…背景に関する符号化ビットストリーム、１１１…人物Ａに関する符号化ビットストリーム、１１２…人物Ｂに関する符号化ビットストリーム、１１３、３０４、５０６…データ多重化部、１１４…多重化ビットストリーム、２０１…Content-based codingに基づく画像情報の受信・読み出し装置、２０２、４０２、６０２…データ分割部、２０３、２０４、２０５…画像復号化部、２０６…画像信号合成部、２０７…再生画像出力、３０１…暗号化機能を持つContent-based codingに基づく画像情報の送信・記録装置、３０２…暗号化部、３０３…人物Ｂに関する暗号化された符号化ビットストリーム、３０５、５０７…暗号化された多重化ビットストリーム、３０６…暗号化のための鍵情報、４０１…暗号解除機能を持つContent-based codingに基づく画像情報の受信・読み出し装置、４０３…暗号解除部、４０４…暗号を解くための鍵情報、５０１…対象物体を切り換えるながら暗号化を行う機能を持つＣｏｎｔｅｎｔ－ｂａｓｅｄ　ｃｏｄｉｎｇに基づく画像情報の送信・記録装置、５０２、６０３…ビットストリーム切り換えスイッチ、５０３、５０４、５０５…暗号化の適用／不適用を切り換えた符号化ビットストリーム、６０１…対象物体を切り換えるながら暗号解除を行う機能を持つＣｏｎｔｅｎｔ－ｂａｓｅｄ　ｃｏｄｉｎｇに基づく画像情報の受信・読み出し装置。

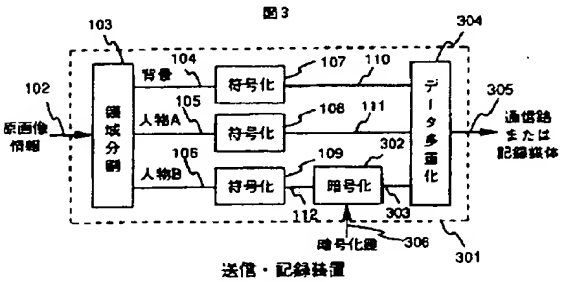
【図１】



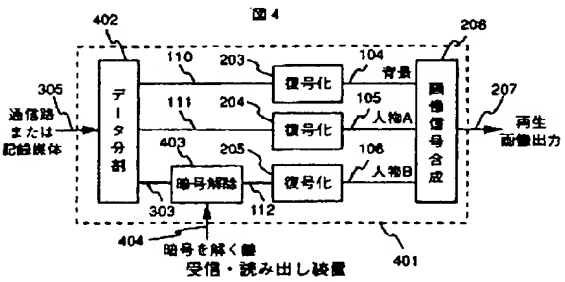
【図２】



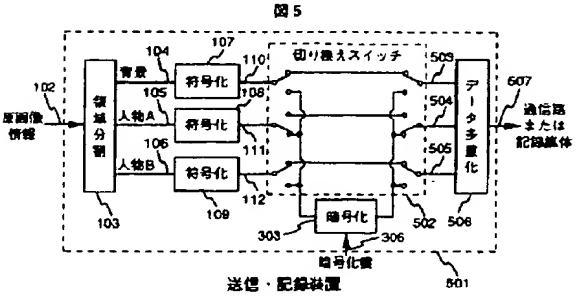
【図３】



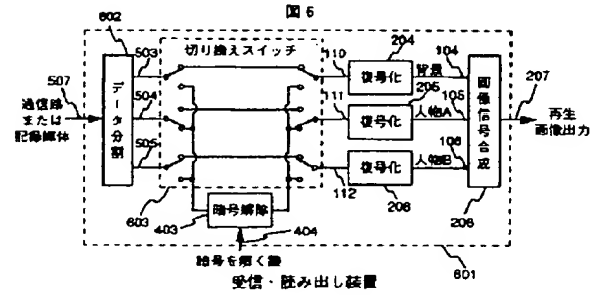
【図４】



【図５】



【図６】



【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１４年３月１５日（２００２．３．１５）

【公開番号】特開平１０－１１２８５１
【公開日】平成１０年４月２８日（１９９８．４．２８）
【年通号数】公開特許公報１０－１１２９
【出願番号】特願平８－２６５７４０
【国際特許分類第７版】
H04N 7/167
H04L 9/36
H04N 7/24
【ＦＩ】
H04N 7/167 Z
H04L 9/00 685
H04N 7/13 Z

【手続補正書】
【提出日】平成１３年１０月１日（２００１．１０．１）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】
【発明の名称】画像情報の伝送または記録方法、装置及びシステム
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】原画像情報に対して画像内の物体ごとに独立に符号化処理を行い、特定の１個または複数の物体に関する符号化ビットストリームのみに暗号化の処理を加えた後に全物体に関する符号化ビットストリームを多重化して出力することを特徴とする画像情報の伝送または記録方法。
【請求項２】請求項１の方法に従って出力された画像情報を受信または読み出して再生する際に、暗号化されていない符号化ビットストリームは正しく再生するが、暗号化された符号化ビットストリームは暗号を解く鍵がないと正しく再生することができないことを特徴とする画像再生方法。
【請求項３】原画像情報に対して画像内の物体ごとに独立に符号化処理を行う手段と、情報に対して暗号化処理を行う手段を持ち、上記符号化手段によって符号化された情報の中で特定の１個または複数の物体に関する符号化ビットストリームのみに暗号化の処理を加えた後に全物体に関する符号化ビットストリームを多重化して出力することを特徴とする画像情報の伝送または記録装置。
【請求項４】請求項１の方法に従って出力された画像情報を受信または読み出して再生する手段と、暗号化された情報を暗号を解く鍵を用いて再生する手段を持ち、暗号化されていない符号化ビットストリームに対応する物体は正しく再生するが、暗号化された符号化ビットストリームに対応する物体は鍵がないと正しく再生することができないことを特徴とする画像再生装置。
【請求項５】物体の符号化ビットストリームに暗号化の処理を加える際に、対象となる物体を切り換えられることを特徴とする請求項３に記載の画像情報の伝送または記録装置。
【請求項６】請求項５に記載の画像情報の伝送または記録方法にしたがって出力された情報に対し、暗号解除の処理を加える符号化ビットストリームを切り換えることによって暗号化された符号化ビットストリームに対応する物体を正しく再生することができることを特徴とする請求項４に記載の画像再生装置。
【請求項７】請求項３または５に記載の画像情報の伝送または記録装置と、請求項４または６に記載の画像再生装置によって構成される画像の通信または放送またはデータベースまたはビデオオンデマンドシステム。
【請求項８】物体に関する符号化ビットストリームの中で暗号化されている物体の数の上限が規定されていることを特徴とする請求項７記載の画像の通信または放送またはデータベースまたはビデオオンデマンドシステム。